Department of Homeland Security Daily Open Source Infrastructure Report for 02 August 2006

Current Nationwide Threat Level is
ELEVATED
Significant Risk of Terrorist Attacks
For info click here
http://www.dhs.gov/

Daily Highlights

- The National Ledger reports power grids in the Midwest, New York, and the Mid−Atlantic are expected to strain but not break from the record−high summer heat on Tuesday and Wednesday, August 1−2. (See item 1)
- The Orlando Sentinel reports a CSX freight train jumped off the tracks after hitting a piece of railroad equipment deliberately left on the tracks, opening up a criminal investigation. (See item 11)
- The Departments of Justice and Homeland Security announced on Monday, July 31, there would be additional resources including federal prosecutors to aid the enforcement of immigration laws and border security along the Southwest border. (See item 16)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://www.esisac.com]

1. *August 01, National Ledger* — **Heat wave blasts Midwest, pushes east and tests power grids.** Power grids in the Midwest, New York, and the Mid−Atlantic are expected to strain but not break during Tuesday and Wednesday, August 1−2, of high summer heat, officials at the various grids said. But unexpected major power plant outages or transmission line breakdowns

could cause rolling blackouts. The heat is now pushing east and causing concern for the grids on Tuesday and Wednesday in New York and the Mid−Atlantic, power grid officials said. The biggest power grid in the United States, PJM, expected to set a record for power use on Tuesday, at about 143,000 megawatts, said Ray Dotter, PJM spokesperson. That would eclipse the mark set July 17 of 139,746 megawatts. The eastbound heat wave pushing temperatures in Eastern cities to the upper 90s to over 100 degrees Fahrenheit with humidity making it feel 110 degrees will last at least through Wednesday.
Source: http://www.nationalledger.com/artman/publish/article_2726740 5.shtml

2. *July 31, Toledo Blade (OH)* — **Fire alarms set off in error evacuate building at Fermi II.** As many as 50 Fermi II workers were evacuated Monday, July 31, from the auxiliary building that sits between the nuclear plant's reactor and the building that houses its steam generators. Fire alarms apparently were errantly triggered on and off by the region's extreme humidity, said Viktoria Mitlyng, Nuclear Regulatory Commission (NRC) spokesperson. No smoke or fire was detected, nor were any injuries or property damage reported. Eileen Dixon, Detroit Edison Co. spokesperson, said the plant's fire brigade responded. She said the utility notified the NRC of an "unusual event" in progress at 1:44 p.m. EDT. The utility hopes to have Fermi II's reactor back at full power late Tuesday night.
Source: http://toledoblade.com/apps/pbcs.dll/article?AID=/20060731/N EWS08/307310019

3. *July 31, News Channel 6 (ID)* — **Substation explosion kills power.** A third of Idaho Falls, ID, was in the dark Monday, July 31, after an explosion at a power substation. The outage affected over 8,000 homes and businesses. At about 12:45 this afternoon, there was an explosion at the West Side Substation and one of the insulators was blown off. The explosion cut off power at four other substations, leaving homes and business from Sunnyside Road to 7th Street without power. Idaho Falls Power was able to reroute power through other substations, and electricity was restored to the area just an hour and a half later. The substation is still out of service, and Idaho Falls Power is waiting for the Bonneville Power Association to make the needed repairs at the substation. No more outages are expected.
Source: http://www.kpvi.com/index.cfm?page=nbcstories.cfm&ID=2969

4. *July 30, Associated Press* — **Fire threatening power lines at Oregon border nearly contained.** A wildfire near the California−Oregon border that threatened a series of major power lines was almost fully contained Sunday, July 30. The blaze in the Shasta−Trinity National Forest, dubbed the Lakin fire, was threatening power lines used by the California−Oregon Transmission Project, the Western Area Power Administration and Pacific Gas & Electric Co. Together, they carry about 4,200 megawatts between Washington's Bonneville Power Administration and California. That threat was greatly diminished by Sunday evening, when officials reported 95 percent containment. However, erratic winds fanning the flames again still could harm the lines, said Cory Hoogendam of the U.S. Forest Service. The California Independent System Operator has said it had contingency plans to reroute electricity around the transmission lines if they failed or had to be shut down because of the fire. The lightning−sparked fire, which has burning more than 500 acres since it started Wednesday, July 26, was expected to be fully contained by Tuesday night, August 1.
Source: http://www.mercurynews.com/mld/mercurynews/news/local/states /california/northern_california/15161073.htm

[Return to top]

Chemical Industry and Hazardous Materials Sector

Nothing to report.
[Return to top]

Defense Industrial Base Sector

5. *July 31, U.S. Air Force* — **Handbook helps weapon systems get to warfighter quicker.** The Department of Defense (DoD) is constantly looking for ways to reduce the time it takes to get new weapon systems in the hands of the warfighter. The acquisition community at Headquarters Air Force Materiel Command is helping the DoD do just that. The acquisition logistics division recently rolled out a new handbook for program managers called the Independent Logistics Assessment, or ILA. The handbook is an optional tool to help program managers meet their responsibility to assess or evaluate a program's product support planning efforts. It provides guidance on how to organize, plan, conduct, document and report an independent logistics assessment. The handbook is built around sustainment elements and has checklists that help guide assessors. The checklists can be tailored to a specific acquisition phase and program.
   Source: http://www.af.mil/news/story.asp?id=123024290

6. *July 01, National Defense Magazine* — **Russia's Littoral Combat Ship angles for international sales.** A Russian corvette currently being built to patrol that country's coastal waters may not live up to the technological stature of the U.S. Navy's littoral combat ship (LCS). But it could offer a lower cost alternative to countries that could never afford the LCS, and a potentially attractive choice to nations unable, for security reasons, to acquire weapons from the United States. The Russian Navy patrol vessels −− known as the Steregushchiy class −− could begin to enter service this year, says naval analyst Richard E. Dorn, vice president of AMI International. The Russians are building three ships, although they said they plan to produce up to 20. According to Dorn, once the first three ships enter service domestically, Russia will court international buyers −− particularly India and China, which have huge demands for coastal patrolling. So far, the U.S. ship has not scored any international sales, although talks are under way with Israel, Dorn says. Russia's corvette has emerged as the only serious contender.
   Source: http://www.nationaldefensemagazine.org/issues/2006/July/Russ iaLittoral.htm

[Return to top]

Banking and Finance Sector

7. *August 01, Finextra* — **Commonwealth Bank beefs up ATM security.** The Commonwealth Bank of Australia (CBA) says it is attaching dye packs to all its cash machines following a significant increase in the number of ATM robberies. The dye packs render the cash unusable and stains the criminals and their vehicles with indelible ink. The packs will be installed in all

high risk ATMs this month and will eventually be rolled out to all machines. The packs only come into operation if the machine's security is breached.
Source: http://finextra.com/fullstory.asp?id=15663

8. *July 31, Advocate (LA)* — **Phishing scam targets La Capitol customers.** Online scammers are targeting customers of La Capitol Federal Credit Union, based in Baton Rouge, LA, using an e−mail warning of suspicious accounts and requesting personal information. The e−mail includes a link to a supposedly secure site that looks similar to La Capitol's online banking page. Susan Parry Leake of La Capitol said the credit union has a contract with a firm that renders the phishers' Websites unusable.
Source: http://www.2theadvocate.com/news/business/businesstoday/3458 501.html

9. *July 31, Associated Press* — **Counterfeit money being printed on lesser−value notes.** A scheme has been hatched to pass off counterfeit money for goods and services, according to the U.S. Secret Service. Lower denomination bills are being bleached then reprinted as notes of higher value, using off−the−shelf computer scanners and printers. Secret Service officials say more and more of these bogus notes have shown up at their offices all over the country in recent months. The fakes now make up 90 percent of the $19,000 in counterfeit cash that the Secret Service's Chicago office receives each week. They are sold on the street for 40 or 50 cents on the fake dollar, in a burgeoning black market, said Xavier Morales, supervisor of the Secret Service's Chicago counterfeit squad. "It's not yet a national problem, but they figured it out here," Morales said. The fakes are printed on bleached bills, the finished product is on the real linen and cotton paper used by the Federal Reserve. The technique gives counterfeiters several advantages, including the fact that the paper feels legitimate, according to Morales. Most counterfeit bills that wind up in the hands of Secret Service agents in Chicago are received from banks after being deposited by fast−food outlets or other small businesses.
Source: http://www.belleville.com/mld/belleville/news/state/15162426 .htm

10. *July 31, IT Wire (Australia)* — **Phishing scam targets Microsoft customers.** Internet security firm SurfControl has warned of an e−mail phishing scam that appears to be a message from Microsoft. The e−mail says the user has won a prize from Microsoft that can be claimed by visiting the Microsoft "Resolution Center" and filling out a small form. When clicking on a link in the e−mail, the user is taken to a malicious Website that resembles Microsoft's home page.
Source: http://www.itwire.com.au/content/view/5144/53/

[Return to top]

Transportation and Border Security Sector

11. *August 01, Orlando Sentinel (FL)* — **FBI: Train mishap was deliberate.** A CSX freight train jumped off the tracks after hitting a piece of railroad equipment deliberately left on the tracks, the FBI said. "It's become a criminal investigation," FBI spokesperson Carol Michalik said Monday. July 31. "Something was left on the tracks." No one was hurt when the CSX engine and three cars derailed Sunday evening, July 30. About 200 gallons of diesel fuel spilled from the engine, and a major Tampa road was closed all day Monday as workers cleaned up the mess.

Source: http://www.orlandosentinel.com/news/local/state/orl−train0106aug01,0,218574.story?coll=orl−news−headlines−state

12. *August 01, USA TODAY* — **Northwest flight attendants vote against contract.** Northwest Airlines' flight schedule could begin being disrupted as early as August 15, after flight attendants' rejection Monday, July 31, of a second tentative contract. The country's No. 5 carrier, operating in Chapter 11 bankruptcy since last September, said in response to the union vote that it is unilaterally imposing on flight attendants terms of an earlier tentative agreement. In June, the attendants rejected that first tentative agreement. Mike Becker, Northwest's senior vice president of human resources, said Northwest is using previously granted authority from the bankruptcy court to impose the terms of the rejected deal. The flight attendants' union says the cut in total compensation, considering the reduction in benefits and added work demands, equals 40 percent. Union spokesperson Corey Caldwell initially warned that management's decision to impose those terms on members of the Association of Flight Attendants−Communications Workers of America will trigger the launch of the union's trademark Chaos (which stands for "create havoc around our system") plan at Northwest. Northwest officials previously have said such ministrikes would be illegal and that they would go to court to block or stop such actions.
Source: http://www.usatoday.com/travel/flights/2006−07−31−northwest−flight−attendants_x.htm

13. *August 01, Statesman Journal (OR)* — **Salem to spend $500,000 to expand airport.** Salem, OR, will move quickly to expand its municipal airport, spending as much as a half−million dollars to add a modular building to the air terminal before the end of the year, the Salem City Council voted Monday, July 31. The expansion was prompted by discussions with Delta Airlines and Allegiant Air, said City Manager Bob Wells. "It has become apparent through conversations we have had with two different airlines that we need to be ready when the opportunity comes," Mayor Janet Taylor said. Salem has been lobbying the major airlines to restore commercial air service to McNary Field, which has been without a carrier for 13 years. Business and civic leaders have pressed for the service, calling it essential for the city's future prosperity. The expansion will provide areas at the terminal for security screening, baggage claim, and ticketing, all required by the Federal Aviation Administration. To get air service, the city also will need to secure Transportation Security Administration staff and funding.
Source: http://159.54.226.83/apps/pbcs.dll/article?AID=/20060801/NEWS/608010331/1001

14. *August 01, Federal Computer Week* — **Telecom upgrade causes O'Hare delays.** A configuration problem with a new Federal Aviation Administration (FAA) telecommunications system caused dozens of delayed departures at Chicago's O'Hare International Airport late last week. Two voice lines that link the Terminal Radar Approach Control Facility in Elgin, IL, to the O'Hare tower experienced intermittent connectivity July 27. The lines −− one of which was a backup −− are usually used to coordinate simultaneous aircraft approaches. Because communication was unreliable, FAA officials decided to abandon the technology and switch to an alternate procedure: staggered approaches. FAA officials conducted staggered approaches for 17 hours and 45 minutes. They chose not to troubleshoot the problem immediately, which could have potentially interfered with aviation activity. A preliminary report indicates the incident spurred 81 delayed departures. However, FAA officials say they are unsure of how many flights were delayed because of the technical problem or the severe thunderstorms in the

area.
Source: http://www.fcw.com/article95495−08−01−06−Web

15. *July 31, USA TODAY* — **United reports $119M in profit.** United Airlines on Monday, July 31, reported its first quarterly profit since 2000, the result of strong travel demand, higher fares, and cost cutting. The airline's profit for the second quarter continued the string of positive results from an industry that has seen enormous losses in the past six years. So far American, United, Continental, US Airways, Southwest, Alaska, AirTran, JetBlue, and Frontier have reported profits totaling $1.3 billion for the April−June quarter. From 2000 through 2005, the industry lost more than $40 billion. The only large U.S. carriers not to report yet, Delta and Northwest, are operating in Chapter 11 and are expected to post second−quarter losses. But they, too, have reported significant improvement in monthly reports required by the bankruptcy court. The improved financial performance at United is largely because of the cost cutting done during a 38−month stint in bankruptcy that ended in February. The carrier slashed more than $7 billion in annual costs while in Chapter 11. At the same time, the airline is trying to increase revenue in various ways, including fare increases and tighter limits on the number of deeply discounted seats.
Source: http://www.usatoday.com/travel/flights/2006−07−31−united−pro fits_x.htm

16. *July 31, Department of Homeland Security* — **Federal prosecutors added for U.S./Mexico border districts.** The Departments of Justice and Homeland Security announced on Monday, July 31, additional resources to enhance the enforcement of immigration laws and border security along the Southwest border. The Department of Justice will add 20 Assistant United States Attorneys (AUSAs) to the five federal law enforcement districts along the border: the Southern District of Texas, the Western District of Texas, the District of Arizona, the District of New Mexico, and the Southern District of California. These 20 AUSAs will prosecute only immigration−related offences, including alien smuggling, entering the United States without inspection, illegal re−entry, possession of firearms as an alien, illegal employment of undocumented aliens, human trafficking and document fraud. The additional resources will be funded by a $2 million supplemental appropriation that was requested by the President and approved by Congress. The hiring process will begin immediately. The Department of Justice's Organized Crime Drug Enforcement Task Force Program will provide funding for five new AUSAs −− one in each of the federal districts along the border −− to prosecute drug trafficking organizations responsible for smuggling illegal narcotics across the Southwest border.
Source: http://www.dhs.gov/dhspublic/display?content=5769

17. *July 31, Government Accountability Office* — **GAO−06−903: Coast Guard: Observations on the Preparation, Response, and Recovery Missions Related to Hurricane Katrina (Report).** Hurricane Katrina was one of the largest natural disasters in this nation's history. Significant federal, state, and local resources were mobilized to respond to the Hurricane Katrina disaster, including those of the U.S. Coast Guard. The Coast Guard played a key role in the planning, response, and recovery efforts for Hurricane Katrina in three mission areas: search and rescue, marine pollution response, and management of maritime commerce. This report discusses the activities undertaken by the Coast Guard, as well as the challenges and lessons learned as a result of the agency's efforts. More specifically, it focuses on (1) the factors that prepared the Coast Guard to perform these three mission areas in the aftermath of Hurricane Katrina; (2) the Coast Guard's response to Hurricane Katrina, the challenges it faced in

performing its missions, and its efforts to mitigate these challenges; and (3) the implications and lessons learned, as identified by the Coast Guard, regarding the effect of Hurricane Katrina surge operations on its people, assets, financial resources, and operations. The Government Accountability Office is not making any recommendations in this report.
Highlights: http://www.gao.gov/highlights/d06903high.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−903

[Return to top]

Postal and Shipping Sector

18. *August 01, Reuters* — **FedEx, U.S. Postal Service renew delivery deal.** Package−delivery company FedEx Corp. and the U.S. Postal Service on Tuesday, August 1, said they had renewed through 2013 an agreement for FedEx's FedEx Express unit to transport domestic mail by air. The deal comes just over a month after FedEx's main rival, United Parcel Service Inc. (UPS), announced it had a deal with the U.S. Postal Service increasing the amount of packages it would deliver to more than $100 million annually. FedEx has been far ahead of UPS in hauling packages for the postal service, carrying one billion pounds of mail in 2005 and generating revenue of around $1.3 billion.
Source: http://biz.yahoo.com/rb/060801/transport_fedex_postalservice .html?.v=3

19. *August 01, Rolla Daily News (MO)* — **Suspicious package causes post office lockdown.** A suspicious package in the lobby of the Rolla Post Office caused an employee evacuation and a brief police barricade around the building on Monday morning, July 31. Post office officials discovered an unattended, locked suitcase in the lobby of the building at around 7 a.m. CDT, according to Postmaster Bill Mayfield. It was later discovered by the Rolla Police Department that the suitcase had been left by an individual affiliated with the University of Missouri−Rolla who arrived to mail the package before the post office opened at 7:45 a.m. Upon initial discovery, post office officials treated the package as “suspicious” and evacuated all post office employees before calling the Rolla Police Department. Mayfield said, “This is common practice in any federal building.” It turned out that the individual who left the package was not from the United States and did not understand the significance of leaving a package unattended in the lobby of a federal building.
Source: http://www.therolladailynews.com/articles/2006/08/01/news/ne ws03.txt

[Return to top]

Agriculture Sector

20. *July 31, Reuters* — **Canada anthrax outbreak worst in decades.** Two separate anthrax outbreaks in the Canadian Prairies have killed about 500 animals on an estimated 100 farms, the Canadian Food Inspection Agency (CFIA) said on Monday, July 31, marking some of the worst levels in decades. The CFIA's computer records on anthrax date back only to the 1950s, but Stephens said the number of affected farms in Saskatchewan is the largest in the CFIA's history since then. Anthrax occurs naturally in the Prairies and is a fatal disease caused by a spore−forming bacterium that has been shed by an infected animal. Saskatchewan first reported

cattle dying due to anthrax in late June, following spring flooding. As of Monday, 409 cattle, bison and other livestock had died from the disease with 86 farms quarantined and classified as positive premises. In Manitoba, which borders Saskatchewan, an unrelated anthrax outbreak believed to be caused by hot and dry conditions was first announced on July 20 and has killed 88 animals on 11 farms. The number of fatalities was expected to slow down as thousands of livestock have been vaccinated against the disease. Earlier this month Minnesota, which borders Manitoba to the south, reported its worst outbreak of livestock anthrax in 87 years.
Source: http://today.reuters.co.uk/news/newsArticle.aspx?type=healthNews&storyID=2006-07-31T210615Z_01_N311845_RTRIDST_0_HEALTH-FOOD-CANADA-ANTHRAX-DC.XML&archived=False

[Return to top]

Food Sector

21. *August 01, Agence France-Presse* — **Japan rejects U.S. call for talks on beef restrictions.** Japan's farm minister has said that it was too soon for talks with the U.S. on lifting partial restrictions on beef imports, due to consumer fears over mad cow disease. Japan the week of July 24 ended an import ban on US beef but only for meat from cattle aged up to 20 months, with brain, spinal cord and other risk materials removed before shipment. The U.S. welcomed the resumption but called for talks later this year to raise the age limit to 30 months. Japan, formerly the top market for US beef, has halted US beef imports twice since December 2003 due to mad cow health scares. A U.S. shipment in January contained animal spines, leading Japan abruptly to bar all U.S. beef just one month after it had first lifted the embargo.
Source: http://news.yahoo.com/s/afp/20060801/hl_afp/healthjapanustramadcow_060801111538;_ylt=AmysKJ5w9HrJoTEAFMTyNiiJOrgF;_ylu=X3oDMTA5aHJvMDdwBHNlYwN5bmNhdA--

22. *July 31, Food Safety and Inspection Service* — **Ground beef recalled.** Ray's Wholesale Meats, a White, GA, firm, is voluntarily recalling approximately 120 pounds of ground beef that may be contaminated with E. coli O157:H7, the U.S. Department of Agriculture's Food Safety and Inspection Service (FSIS) announced Monday, July 31. The problem was discovered through routine FSIS microbiological testing. FSIS has received no reports of illnesses associated with consumption of this product. The ground beef was produced on July 25 and was distributed to retail establishments in Georgia. E. coli O157:H7 is a potentially deadly bacterium that can cause bloody diarrhea and dehydration.
Source: http://www.fsis.usda.gov/News_&_Events/Recall_024_2006_Relea se/index.asp

23. *July 31, U.S. Food and Drug Administration* — **Consumers advised to avoid raw oysters from the Pacific Northwest.** The U.S. Food and Drug Administration (FDA) is advising consumers to avoid eating raw oysters harvested in the Pacific Northwest as a result of increased reports of illnesses associated with the naturally occurring bacteria Vibrio parahaemolyticus (Vp) in oysters harvested from the area. Oysters harvested from this region have been reported to cause gastrointestinal illness. In recent months, there has been an unusual increase in bacterial illness associated with eating raw oysters from the Pacific Northwest. The illnesses are associated with the naturally occurring bacterium Vp, which is most prevalent during summer months when water temperatures in the Pacific Northwest are most favorable

for its growth. While Vp can cause mild gastrointestinal disorders in healthy individuals, older persons and those with weak immune systems are at greater risk for serious more illness, such as septicemia (infection of the blood system). Pacific Northwest oysters are distributed nationally. Although to date most of the illnesses reported have occurred in the Pacific Northwest, some have been reported in New York state as well. In Washington state, authorities are identifying and closing areas where people have become sick from eating oysters. Washington state has initiated a recall of all shell stock oysters harvested from areas closed within the state.
Source: http://www.fda.gov/bbs/topics/NEWS/2006/NEW01422.html

[Return to top]

Water Sector

Nothing to report.
[Return to top]

Public Health Sector

24. *August 01, Associated Press* — **Experts urge prudent antibiotic use.** A task force examining the expensive, sometimes−deadly problem of bacteria increasingly becoming resistant to antibiotics says New Jersey hospitals must increase surveillance of these microbes and improve infection control practices. A strategic plan from the task force, released Monday, July 31, also recommends better educating the public about the danger and standardizing testing to determine which antibiotics best kill specific microbes prevalent in a hospital or region, information that can guide doctors' choice of medication. The 30−member task force of health experts, established in February 2005 by the state Department of Health & Senior Services, sets those four steps as goals, along with a fifth: calculating the economic impact of antimicrobial resistance in New Jersey and demonstrating the financial benefits of reducing the problem. Under the strategic plan, hospitals will focus on tracking antibiotic−resistant strains of several bacteria that are common and very dangerous, and reports will be submitted to the state electronically, allowing better analysis. Prisons and long−term acute−care facilities are interested in doing that as well, and the tracking could be expanded to nursing homes, private doctor's offices and home care agencies.
Report: http://www.state.nj.us/health/cd/mrsa/documents/mrsa_strateg ic_plan.pdf
Source: http://www.cbsnews.com/stories/2006/08/01/ap/health/mainD8J7 ABUO0.shtml

25. *August 01, New York Times* — **Researchers explore ways bird flu may spread.** A new study addresses the most urgent public health question about bird flu: what would it take to make the virus more contagious in people? Researchers from the U.S. Centers for Disease Control and Prevention tried to make the A(H5N1) bird flu virus more contagious, but could not. That result may sound like good news, but the scientists urge caution. “These data do not mean H5N1 cannot convert to being transmissible person to person,” said Dr. Julie Gerberding, director of the disease centers. “They mean it is not simple.” Since 2003, the virus spread from Asia to Europe and Africa, infecting millions of birds and some humans, mostly through contact with birds. So far, 232 people in 10 countries have contracted bird flu, and 134 have died. The one

thing that has prevented the disease from causing a human pandemic is its inability to spread easily among people. But that could change. Scientists' biggest fear has been that A(H5N1) may mix with a human flu virus that does spread in people, swap a few genes and morph into a new, highly contagious strain that could cause a deadly pandemic.
Abstract: http://www.pnas.org/cgi/content/abstract/0605134103v1
Source: http://www.nytimes.com/2006/08/01/health/01flu.html?_r=1&ref =health&oref=slogin

26. *August 01, Agence France−Presse* — **Laos starts poultry cull to limit bird flu outbreak.** Laos has started a poultry cull in three villages near the capital Vientiane to limit the spread of the bird flu virus, an official has said. "There is no new outbreak but we have taken measures in a three−mile radius around the farms contaminated," said foreign ministry spokesperson Yong Chanthalangsy on Tuesday, August 1. It was unclear how many animals would be culled. About 19,000 chickens had been destroyed by Sunday, July 30. In late July an outbreak of the H5N1 strain of bird flu killed thousands of chickens at two different sites on a state−owned poultry farm, 15 miles south of Vientiane. It was Laos' first official outbreak of the deadly virus since 2004, although a case involving a single duck was detected earlier this year.
Source: http://news.yahoo.com/s/afp/20060801/hl_afp/healthflulaos_06 0801121243

27. *July 31, CBS 13 (CA)* — **California man dies of hantavirus.** A camping trip in the Sierra has turned tragic for one California family after a man dies from a rare virus. The man died July 14 from hantavirus becoming the first Californian in three years to die of the virus. Health officials believe the 52−year−old was infected near Bridgeport, about 50 miles north of the Mammoth Lakes resort area.
Hantavirus information: http://www.cdc.gov/ncidod/diseases/hanta/hps/index.htm
Source: http://cbs13.com/bios/local_story_212094507.html

[Return to top]

Government Sector

Nothing to report.
[Return to top]

Emergency Services Sector

28. *August 01, Federal Emergency Management Agency* — **Federal Emergency Management Agency National Situation Update.** Tropical Activity: Atlantic/Gulf of Mexico/Caribbean Sea: At 5:00 a.m. EDT Tuesday, August 1, Tropical Storm Chris (formerly Tropical Depression 03) with maximum sustained winds near 40 mph was located near latitude 16.6 north longitude 59.2 west. Some strengthening is forecast during the next 24 hours. Tropical Storm Chris is moving toward the west−northwest near 9 mph. On the forecast track Chris is expected to move over or near the Leeward Islands Tuesday night or early Wednesday morning. At 5:00 a.m. EDT Tuesday, a Tropical Storm Watch was issued for Puerto Rico and the U.S. Virgin Islands and for the British Virgin Islands. Eastern Pacific: At 5:00 a.m. EDT August 1, Tropical Storm Fabio was located near 14.8 north 124.6 west moving towards the west−northwest at 14 mph. Fabio has sustained winds near 40 mph. The storm is expected to eventually lose strength and

become a remnant low.
To view other Situation Updates: http://www.fema.gov/emergency/reports/index.shtm
Source: http://www.fema.gov/emergency/reports/2006/nat080106.shtm

29. *August 01, Reuters* — **Streamlined Indian Ocean tsunami alert crucial.** Indian Ocean nations must shed national pride and ensure a planned regional tsunami warning system is simple enough to work, a top official from the United Nations' science arm said on Tuesday, August 1. After 18 months of work, government weather agencies in almost all members of the Intergovernmental Coordination Group for the Indian Ocean Tsunami Warning and Mitigation System have been connected. However, they still rely on the Japan Meteorological Agency and the U.S. Pacific Tsunami Warning Center for tsunami alerts although both are hubs for the Pacific, not the Indian Ocean. At the current meeting on the resort island of Bali, member states should decide who will host the Indian Ocean hub.
Source: http://www.alertnet.org/thenews/newsdesk/B342130.htm

30. *July 31, CongressDaily* — **FEMA chief details preparations for hurricane season.** Acknowledging numerous problems with the agency's response to Hurricane Katrina last year, Federal Emergency Management Agency (FEMA) Director R. David Paulison on Monday, July 31, described a beefed−up organization that he said would be better able to respond swiftly to the needs of disaster victims during this year's hurricane season. A key aspect of the improvement has been an effort to increase the supplies available for victims −− and FEMA's ability to deliver them. Paulison said that while FEMA had enough equipment on hand during Katrina, it was not in the right position to be useful. FEMA has also vastly increased its supplies of water and ice and doubled its pre−Katrina staff of disaster assistance employees from approximately 4,000 to about 8,000. In addition, FEMA has signed a memorandum of understanding with the Defense Logistics Agency, which will serve as a "backup" to help move supplies, according to Paulison.
Source: http://www.govexec.com/story_page.cfm?articleid=34681&dcn=to daysnews

31. *July 31, Honolulu Advertiser* — **First−responder radio towers in Hawaii being replaced.** A new city analysis of Honolulu shows eight of 24 city radio communications towers must be replaced as part of a $22.5 million project to update the vital network that emergency responders rely on each day. Nearly a year into the effort to upgrade the Oahu emergency system, city information technology director Gordon Bruce said the assessment shows where the weak links are. The city has begun replacing the towers, which continue to operate despite their condition, on a schedule of two to three new towers a year. While the city is spending money to repair the deteriorating towers, workers also have been updating radio technology. The updates have allowed the city to bridge a critical gap that had kept the police and fire departments from communicating directly. As a result of the work, Honolulu is ahead of many cities in terms of interoperability.
Source: http://www.honoluluadvertiser.com/apps/pbcs.dll/article?AID=/20060731/NEWS04/607310331/1008/NEWS

[Return to top]

Information Technology and Telecommunications Sector

32. *August 01, Register (UK)* — **Worm targets Windows PowerShell script.** Virus writers have created an experimental form of malware written in Windows PowerShell script, the command line and scripting language used by Windows. Cibyz was developed by the same Austrian VXers who developed proof of concept malware targeting Microsoft Command Shell (MSH) technology, later renamed PowerShell. Cibyz represents a refinement of earlier malware that's capable of infecting Windows XP and Windows Server 2003 machines, as well as Vista boxes.
For further detail: http://vil.nai.com/vil/content/v_140292.htm
Source: http://www.channelregister.co.uk/2006/08/01/powershell_worm/

33. *July 31, FrSIRT* — **Apple Safari "KHTMLParser::popOneBlock()" client side memory corruption vulnerability.** A vulnerability has been identified in Apple Safari, which could be exploited by remote attackers to crash a vulnerable browser or take complete control of an affected system. Analysis: This issue is due to a memory corruption error in the "KHTMLParser::popOneBlock()" function when handling a script element in a div object redefining the document body, which could be exploited by attackers to cause a denial−of−service or execute arbitrary commands by convincing a user to visit a specially crafted Webpage.
Affected Products: Apple Safari version 2.0.4 (419.3) and prior.
Solution: The FrSIRT is not aware of any official supplied patch for this issue.
Source: http://www.frsirt.com/english/advisories/2006/3069

34. *July 31, Security Focus* — **Firm classifies flaws to help developers.** Security firm Fortify announced on Monday, July 31, that the firm had created a hierarchy for labeling security issues in hopes that giving names to software flaws will enable programmers to avoid making the same mistakes. The hierarchy consists of 115 categories split among seven "kingdoms" or top−level classes and a catch−all external class. The top−level seven kingdoms are input validation and representation, API abuse, security features, time and state, errors, code quality, and encapsulation. Fortify also announced on Monday that the firm had donated the research project to the Open Web Application Security Project.
Source: http://www.securityfocus.com/brief/267

35. *July 31, Associated Press* — **McAfee Security programs may expose data.** Consumer versions of McAfee Inc.'s leading software for securing PCs is susceptible to a flaw that can expose passwords and other sensitive information stored on personal computers, researchers said Monday, July 31. The vulnerability affects many of McAfee's most popular consumer products, including its Internet Security Suite, SpamKiller, Privacy Service and Virus Scan Plus titles, said Marc Maiffret, chief hacking officer at eEye Digital Security Inc. McAfee spokesperson Siobhan MacDermott confirmed the vulnerability and said software engineers were testing a fix. She said officials expected to release the patch Wednesday, August 2, using a feature that automatically updates McAfee products over the Internet.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2006/07/31/AR2006073101195.html

36. *July 31, Security Focus* — **Multiple Microsoft vulnerabilities reported.** Microsoft PowerPoint is prone to an unspecified code execution vulnerability. Analysis: A proof of concept exploit file designed to trigger this vulnerability has been released. This issue arises when a vulnerable user opens a malicious read only PowerPoint file and then closes it. It is

currently unknown if this exploit file pertains to a newly discovered, unpublished vulnerability.
For further detail: http://www.securityfocus.com/bid/19229/discuss
Microsoft Internet Explorer is prone to a denial−of−service vulnerability. This issue is triggered when an attacker convinces a victim user to visit a malicious Website. Analysis: Remote attackers may exploit this issue to crash Internet Explorer, effectively denying service to legitimate users.
For further detail: http://www.securityfocus.com/bid/19228/discuss
Reportedly, the Microsoft Windows GDI+ library 'gdiplus.dll' is prone to a denial−of−service vulnerability because the software fails to handle malformed image files properly. Analysis: An attacker may leverage this issue to trigger a denial−of−service condition in software implementing the vulnerable library. Other attacks may also be possible.
For further detail: http://www.securityfocus.com/bid/19221/discuss
Microsoft Windows is reportedly prone to a remote denial−of−service vulnerability because the operating system fails to properly handle network traffic. Analysis: This issue may cause affected computers to crash, denying service to legitimate users.
For further detail: http://www.securityfocus.com/bid/19215/discuss
Source: http://www.securityfocus.com/vulnerabilities

37. *July 31, eWeek* — **Net turns up a second burned Dell Notebook.** Dell says it's investigating a report of a second laptop fire. The Round Rock, TX, PC maker says it's working to gain possession of a machine which melted itself at a Vernon Hills, IL, company Tuesday, July 25. A company employee posted pictures and a description of the incident, in which he said the machine's battery burned, on Tom's Hardware Forumz. The Illinois incident follows that of a machine that went up in smoke at a business conference in Japan in late May.
Pictures: http://www.tgdaily.com/picturegalleries/gallery−20060731−1.h tml
Source: http://www.eweek.com/article2/0,1895,1996800,00.asp

38. *July 28, EE Times* — **DDoS attack may be behind MySpace, AOL problems.** Multiple proprietary Web−based services experienced simultaneous log−in problems shortly after 11 a.m. EDT on Friday, July 28, raising the possibility that a distributed denial−of−service (DDoS) attack was underway. America Online (AOL), MySpace.com and Earthlink all had problems with user log ins, and with access to home page or archived e−mail accounts.
Source: http://www.eetimes.com/news/latest/showArticle.jhtml?article ID=191600001

39. *July 28, CNET News* — **JavaScript opens doors to browser−based attacks.** Security researchers have found a way to use JavaScript to map a home or corporate network and attack connected servers or devices, such as printers or routers. The malicious JavaScript can be embedded in a Webpage and will run without warning when the page is viewed in any ordinary browser, the researchers said. It will bypass security measures such as a firewall because it runs through the user's browser, they said. "We have discovered a technique to scan a network, fingerprint all the Web−enabled devices found and send attacks or commands to those devices," said Billy Hoffman, lead engineer at Web security specialist SPI Dynamics. "This technique can scan networks protected behind firewalls such as corporate networks." A successful attack could have significant impact.
Source: http://news.com.com/JavaScript+opens+doors+to+browser−based+ attacks/2100−7349_3−6099891.html?tag=cd.lede

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US−CERT Operations Center Synopsis: US−CERT has received information that a website on the Internet is hosting malicious software that has been or is currently being used to compromise systems.

IP: 211.34.248.244

Activity:
This activity is similar to what was reported on July 6th concerning the "beststartmotor" domain. The original email stated: "In April 2006, users reported having their web browsers redirected from other websites to the domain beststartmotor.com using an HTML command called an iframe. Once redirected, the victim's web browsers usually download malware onto the victim's computer." Currently, another website may have a similar iframe link to IP 211.34.248.244. Once a web browser on a victim system follows this link, the victim computer may download malware which can compromise that computer.

Recommendation:
US−CERT suggests that each agency evaluate the potential risk and take protective measures in a manner that is consistent with the agency's policies and procedures. Please refrain from investigating / visiting the IP address as this may result in accidental infection of your computer. Please be advised that the IP address listed above may also host additional domains and websites. However, this information is being shared to allow the GFIRST community to understand the potential risk associated with those domains.

US−CERT requests that all agencies examine firewall, web proxy and other network perimeter device logs for suspicious traffic to and from the above IP. Should you encounter such activity, please notify US−CERT at soc@us−cert.gov or via phone at 888−282−0870.

Active Exploitation of a Vulnerability in Microsoft PowerPoint
US−CERT is aware of active exploitation of a new vulnerability in Microsoft PowerPoint. Successful exploitation could allow a remote attacker to execute arbitrary code with the privileges of the user running PowerPoint.

For more information please review the following vulnerability note:

VU#936945: Microsoft PowerPoint contains an unspecified remote code execution vulnerability. http://www.kb.cert.org/vuls/id/936945

US−CERT strongly encourages users not to open unfamiliar or unexpected email attachments, even if sent by a known and trusted source. Users may wish to read Cyber Security Tip ST04−010 for more information on working with email attachments. http://www.us−cert.gov/cas/tips/ST04−010.html

US−CERT will continue to update current activity as more information becomes available.

PHISHING SCAMS

US−CERT continues to receive reports of phishing scams that target online users and Federal government web sites. US−CERT encourages users to report phishing incidents based on the following guidelines:

Federal Agencies should report phishing incidents to US−CERT.
http://www.us−cert.gov/nav/report_phishing.html

Non−federal agencies and other users should report phishing incidents to Federal Trade Commissions OnGuard Online. http://onguardonline.gov/phishing.html

Current Port Attacks

Top 10 Target Ports	1026 (win−rpc), 41170 (−−−), 4672 (eMule), 25 (smtp), 27164 (−−−), 38566 (−−−), 445 (microsoft−ds), 24232 (−−−), 6881 (bittorrent), 80 (www) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

40. *August 01, WUSA9 (DC)* — **National Night Out.** The annual National Night Out is sponsored by the National Association of Town Watch (NATW). The evening is designed to generate neighborhood support and participation in crime prevention efforts and to enhance police and community relations. Along with the traditional display of outdoor lights and front porch vigils, many communities celebrate with a variety of events to help neighbors get to know one another, build community spirit, and demonstrate a community's commitment to keep neighborhoods free from crime. Washington, DC's celebration will begin at 5 p.m. EDT with a citywide kickoff ceremony where Mayor Tony Williams and Police Chief John Ramsey will be joined by leaders from the community and government agencies. The kickoff event will be followed by dozens of neighborhood crime prevention events in all seven police districts.
NATW Website: http://www.nationalnightout.org/natw
Source: http://www.wusatv9.com/news/news_article.aspx?storyid=51016

[Return to top]

General Sector

Nothing to report.
[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

Department of Homeland Security Disclaimer